B

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,846	10/14/2003	James R. Giles	YOR20030518US1(590.122)	8448

35195 7590 04/04/2007
FERENCE & ASSOCIATES LLC
409 BROAD STREET
PITTSBURGH, PA 15143

EXAMINER	
SHAW, YIN CHEN	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	**Applicant(s)**	
Office Action Summary	10/685,846	GILES ET AL.	
	Examiner	**Art Unit**	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2003*.
2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-29* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on *10/14/2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a)☐ All b)☐ Some * c)☐ None of:
1.☐ Certified copies of the priority documents have been received.
2.☐ Certified copies of the priority documents have been received in Application No. _____.
3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

AU2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 have been submitted for examination.
2. Claims 1-29 have been examined and rejected.,
3. Rejections of Independent claims are provided with detailed citations from the prior arts.

Claim Objection

4. Claim 13 is objected for failing to provide an antecedent basis for the claimed the recited limitation "transferring the protected key". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 5, 7, 19, and 25-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Engberg et al. (U.S. Patent 6,993,658).

    a. *Referring to Claims 1, 25, and 27:*

    As per Claim 1, Engberg et al. disclose a method of enabling at least one pervasive device to retrieve at least one authentication token from at least one personal authentication gateway, the at least one pervasive device comprising at least one automatic token client application and the at least one personal authentication gateway comprising at least one token server application, said method comprising the steps of: ascertaining at least one personal authentication gateway from the at least one pervasive device **[(lines 13-17, Col. 4 and lines 27-32, Col. 6)]**;

    sending at least one token request from at least one pervasive device to at least one personal authentication gateway **[(lines 22-25 and 58-60, Col. 5; Fig. 1)]**; and

    receiving a token response at the pervasive device from the at least one personal authentication gateway **[(lines 28-31 and 60-65, Col. 5; Fig. 1)]**.

    As per Claim 25, it is a program storage device claim that corresponds to the method claim 1. Therefore, it is rejected with the same rationale applied against Claim 1 above.

As per Claim 27, it is a computer usable medium claim that corresponds to the method claim 1. Therefore, it is rejected with the same rationale applied against Claim 1 above.

b. *Referring to Claim 5:*

As per Claim 5, Engberg et al. disclose the method according to claim 1, wherein said receiving step comprises storing received credentials for use by other applications **[(lines 17-25, Col. 4 and lines 38-43, Col. 7; Fig. 2)]**.

c. *Referring to Claims 7, 26, and 28:*

As per Claim 7, Engberg et al. disclose a method of enabling at least one personal authentication gateway to distribute at least one authentication token to at least one authorized pervasive device, the at least one personal authentication gateway comprising at least one token server and the at least one pervasive device comprising at least one automatic token client, said method comprising the steps of:

receiving at least one token request from at least one pervasive device on at least one personal authentication gateway **[(lines 22-25 and 58-60, Col. 5; Fig. 1)]**;

determining whether the pervasive device is authorized to receive authentication tokens **[(lines 36-42, Col. 6)]**; and sending at least one token response to the at least one pervasive device from at least one personal authentication gateway **[(lines 28-31 and 60-65, Col. 5; Fig. 1)]**.

As per Claim 26, it is a program storage device claim that corresponds to the method claim 7. Therefore, it is rejected with the same rationale applied against Claim 7 above.

As per Claim 28, it is a computer usable medium claim that corresponds to the method claim 7. Therefore, it is rejected with the same rationale applied against Claim 7 above.

d. *Referring to Claims 19 and 29:*

As per Claim 19, Engberg et al. disclose an apparatus for enabling at least one pervasive device to retrieve at least one authentication token from at least one personal authentication gateway, said apparatus comprising:

a discoverer which finds at least one personal authentication gateway capable of responding to token requests **[(lines 13-17, Col. 4 and lines 27-32, Col. 6)]**;

a token requestor which sends at least one requests for at least one token required by the at least one pervasive device **[(lines 22-25 and 58-60, Col. 5; Fig. 1)]**; and a token responder which accepts at least one token requests and sends at least one token response with at least one authentication token to at least one authorized pervasive device **[(lines 22-25, 28-31, and 60-65, Col. 5; Fig. 1)]**.

As per Claim 29, it is a computer usable medium claim that corresponds to the method claim 19. Therefore, it is rejected with the same rationale applied against Claim 19 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-3, 6, 8-10, 12, 15-18, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Engberg et al. (U.S. Patent 6,993,658) and further in view of Traversat et al. (U. S. Pub. 2002/0152299).

   a. *Referring to Claim 2:*

   As per Claim 2, Engberg et al. disclose the method according to claim 1. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Traversat et al. disclose wherein said ascertaining step comprises broadcasting a pervasive authentication domain discovery request message and receiving at least one discovery response message from the at least one personal authentication gateway **[(lines 1-3 of [0277]; lines 1-10 of [0323]; lines 9-18 of [0331] from Traversat et al.)]**.

Engberg et al. and Traversat et al. are from similar technology relating to security for the digital content and token data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Traversat et al. to have the discovery message broadcasting and responding capability since one would be motivated to establish a reliable connections between peers (lines 2-3 of [0007] from Traversat et al.). Therefore, it would have been obvious to combine Engberg et al. with Traversat et al. to obtain the invention as specified in claim 2.

b. *Referring to Claim 3:*

As per Claim 3, Engberg et al. disclose the method according to claim 1. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Traversat et al. disclose wherein said ascertaining step comprises looking up a personal authentication gateway address in configuration settings **[(lines 6-8 of [0163]; lines 5-6 of [0322]; lines 1-9 of [0343]; lines 9-10 of [0344] from Traversat et al.)]**.

Engberg et al. and Traversat et al. are from similar technology relating to security for the digital content and token data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Traversat et al. to have the capability to look up an address for an entity peer since one would be motivated to establish a reliable connections between peers (lines 2-3 of [0007] from Traversat et al.). Therefore, it would have been obvious to combine Engberg et al. with Traversat et al. to obtain the invention as specified in claim 3.

c. *Referring to Claim 6:*

As per Claim 6, Engberg et al. disclose the method according to claim 1. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Traversat et al. disclose the step of registering a pervasive device to be a member of a pervasive authentication domain by registering with a personal authentication gateway **[(lines 1-3 of [0053] and lines 1-10 and 19-21 of [0482] from Traversat et al.)]**. Engberg et al. and Traversat et al. are from similar technology relating to security for the digital content and token data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Traversat et al. to have the pervasive device as a peer member in the domain group since one would be motivated to establish a reliable connections between peers (lines 2-3 of [0007] from Traversat et al.). Therefore, it would have been obvious to combine Engberg et al. with Traversat et al. to obtain the invention as specified in claim 6.

d. *Referring to Claim 8:*

As per Claim 8, Engberg et al. disclose the method according to claim 7. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Traversat et al. disclose wherein said sending step comprises the at least one personal authentication gateway responding to a pervasive authentication domain discovery message from the at least one pervasive device **[(lines 1-3 of [0277]; lines 1-10 of [0323]; lines 9-18 of [0331] from Traversat et al.)]**.

Engberg et al. and Traversat et al. are from similar technology relating to security for the digital content and token data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Traversat et al. to have the discovery message broadcasting and responding capability since one would be motivated to establish a reliable connections between peers (lines 2-3 of [0007] from Traversat et al.). Therefore, it would have been obvious to combine Engberg et al. with Traversat et al. to obtain the invention as specified in claim 8.

e. *Referring to Claim 9:*

As per Claim 9, Engberg et al. and Traversat et al. disclose the method according to claim 8, wherein:

said at least one personal authentication gateway has a pervasive authentication domain **[(lines 1-10 of [0482] and Fig. 1 from Traversat et al.)]**;

sending step comprises sending the at least one token response **[(lines 28-31 and 60-65, Col. 5; Fig. 1 from Engberg et al.)]** only if the pervasive device identification for the pervasive authentication domain discovery message is a member of the pervasive authentication domain of the at least one personal authentication gateway **[(lines 1-7 of [0325]; lines 1-3 of [0053]; lines 1-10 and 19-21 of [0482] from Traversat et al.)]**.

f. *Referring to Claim 10:*

As per Claim 10, Engberg et al. disclose the method according to claim 7, wherein said receiving step comprises:

determining the pervasive device identification of the at least one token request **[(lines 36-42, Col. 6)]**;

retrieving at least one authentication token for the pervasive device **[(lines 28-31 and 60-65, Col. 5; Fig. 1)]**.

Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Traversat et al. disclose deriving at least one pervasive authentication domain for the at least one pervasive device **[(lines 1-4 of [0023]; lines 1-10 and 19-21 of [0482]; Fig. 1B from Traversat et al.)]**.

Engberg et al. and Traversat et al. are from similar technology relating to security for the digital content and token data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Traversat et al. to have the pervasive (mobile) device as a member for a peer since one would be motivated to establish a reliable connections between peers (lines 2-3 of [0007] from Traversat et al.). Therefore, it would have been obvious to combine Engberg et al. with Traversat et al. to obtain the invention as specified in claim 10.

g. *Referring to Claim 12:*

As per Claim 12, Engberg et al. disclose the method according to claim 7. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Traversat et al. disclose the step of registering a pervasive device to be a member of a pervasive authentication domain by registering with a personal authentication gateway **[(lines 1-4 of [0023]; lines 1-10 and 19-21 of [0482]; Fig. 1B from Traversat et al.)]**. Engberg et al. and Traversat et al. are from similar technology relating to security for the digital content and token data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Traversat et al. to have the pervasive (mobile) device registered as a member for a peer group (lines 2-3 of [0007] from Traversat et al.). Therefore, it would have been obvious to combine Engberg et al. with Traversat et al. to obtain the invention as specified in claim 12.

h. *Referring to Claim 15:*

As per Claim 15, Engberg et al. and Traversat et al. disclose the method according to claim 10, wherein said determining step comprises validating that the at least one pervasive device has been registered for the at least one pervasive authentication domain **[(lines 1-10 of [0323] and lines 1-13 of [0482]; Fig. 1B from Traversat et al.)]**.

i. *Referring to Claim 16:*

As per Claim 16, Engberg et al. and Traversat et al. disclose the method according to claim 10. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Traversat et al. disclose wherein said determining step comprises ascertaining whether the at least one pervasive device is within a given distance of the at least one personal authentication gateway **[(lines 1-7 of [0301] and lines 1-10 of [0323] from Traversat et al.)]**.

j. *Referring to Claim 17:*

As per Claim 17, Engberg et al. and Traversat et al. disclose the method according to claim 10, wherein said determining step comprises ascertaining whether the at least one pervasive device has recently made a previous request **[(lines 1-6 of [0303] and lines 4-6 of [0417] from Traversat et al.)]**.

k. *Referring to Claim 18:*

As per Claim 18, Engberg et al. and Traversat et al. disclose the method according to claim 10, wherein said determining step comprises ascertaining whether the at least one pervasive device has not sent a message indicating that the at least one pervasive device is no longer to be trusted **[(lines 8-9 of [0112] and lines 1-11 of [0392] from Traversat et al.)]**.

l. *Referring to Claim 24:*

As per Claim 24, Engberg et al. disclose an apparatus comprising means for enabling at least one personal authentication gateway to distribute authentication tokens to at least one authorized pervasive device, said apparatus comprising:

means for receiving a token request from at least one pervasive device **[(lines 22-25 and 58-60, Col. 5; Fig. 1)]**;

means for determining whether the at least one pervasive device is authorized to receive authentication tokens **[(lines 36-42, Col. 6)]**; and

means for sending at least one token response to said at least one pervasive device from at least one personal authentication gateway **[(lines 28-31 and 60-65, Col. 5; Fig. 1)]**.

Engberg et al. do not expressly disclose means for registering at least one pervasive device for membership in a pervasive authentication domain. However, Traversat et al. disclose registering a device as a peer in the pervasive peer domain **[(lines 1-4 of [0023]; lines 1-10 and 19-21 of [0482]; Fig. 1B from Traversat et al.)]**. Engberg et al. and Traversat et al. are from similar technology relating to security for the digital content and token data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Traversat et al. to have the mobile device as a peer device registered in a pervasive peer group since one would be motivated to establish a reliable connections between peers (lines 2-3 of [0007] from Traversat et al.). Therefore, it would have been obvious to combine Engberg et al. with Traversat et al. to obtain the invention as specified in claim 24.

7. Claims 4, 11, and 20-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Engberg et al. (U.S. Patent 6,993,658) and further in view of Lincke et al. (U.S. Patent 6,253,326).

   a. *Referring to Claim 4:*

      As per Claim 4, Engberg et al. disclose the method according to claim 1, wherein the at least one token request comprises a pervasive device identification, a message type **[(lines 32-50, Col. 5 from Engberg et al.)]**. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Lincke et al. disclose a protection arrangement for fields of the at least one token request, the protection arrangement being adapted to ensure integrity and confidentiality as request message being encrypted for security **[(lines 57-62, Col. 89 from Lincke et al.)]**. Engberg et al. and Lincke et al. are from similar technology relating to security for the digital content and data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Lincke et al. to have encrypted request for protection since one would be motivated to securely transmitting a message from a wireless client (lines 38-39, Col. 3 from Lincke et al.). Therefore, it would have been obvious to combine Engberg et al. with Lincke et al. to obtain the invention as specified in claim 4.

b. *Referring to Claim 11:*

As per Claim 11, Engberg et al. disclose the method according to claim 7, wherein the at least one token response sent comprises of a pervasive device identification, the message type, authentication tokens **[(lines 29-32 and 35-40, Col. 6 from Engberg et al.)]**. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Lincke et al. disclose a protection arrangement for fields of the at least one token response, the protection arrangement being adapted to ensure integrity and confidentiality as response message being encrypted for security **[(lines 44-50, Col. 89 from Lincke et al.)]**. Engberg et al. and Lincke et al. are from similar technology relating to security for the digital content and data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Lincke et al. to have encrypted response for protection since one would be motivated to securely transmitting a message from a wireless client (lines 38-39, Col. 3 from Lincke et al.). Therefore, it would have been obvious to combine Engberg et al. with Lincke et al. to obtain the invention as specified in claim 20.

c. *Referring to Claim 20:*

As per Claim 20, Engberg et al. disclose the apparatus according to claim 19, wherein the at least one token request comprises a pervasive device identification, the message type, at least one authentication token **[(lines 29-32 and 35-40, Col. 6 from Engberg et al.)]**. Engberg et al. do not expressly disclose the remaining limitation of the claim. However, Lincke et al. disclose a protection arrangement for fields of the at least one token request, the protection arrangement being adapted to ensure integrity and confidentiality as request message being encrypted for security **[(lines 57-62, Col. 89 from Lincke et al.)]**. Engberg et al. and Lincke et al. are from similar technology relating to security for the digital content and data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Lincke et al. to have encrypted request for protection since one would be motivated to securely transmitting a message from a wireless client (lines 38-39, Col. 3 from Lincke et al.). Therefore, it would have been obvious to combine Engberg et al. with Lincke et al. to obtain the invention as specified in claim 20.

d. *Referring to Claim 21:*

As per Claim 21, Engberg et al. and Lincke et al. disclose the apparatus according to claim 20, wherein said protection arrangement comprises Triple-DES encryption using a long key **[(lines 65-67, Col. 3 and lines 45-50, Col. 91 from Lincke et al.)]**.

e. *Referring to Claim 22:*

As per Claim 22, Engberg et al. and Lincke et al. disclose the apparatus according to claim 21, wherein said long key is a secure hash comprised of a master secret known only to the personal authentication gateway, a pervasive device identification, and a pervasive authentication domain identification **[(lines 9-13, Col. 4; lines 17-22 and 35-38, Col. 6 from Engberg et al.) and (lines 19-21, Col. 85 from Lincke et al.)]**.

f. *Referring to Claim 23:*

As per Claim 23, Engberg et al. and Lincke et al. disclose the apparatus according to claim 21, wherein said long key is distributed to the at least one pervasive device during registration **[(lines 47-49, Col. 85 and lines 45-50, Col. 91 from Lincke et al.)]**.

8. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Engberg et al. (U.S. Patent 6,993,658) and Traversat et al. (U. S. Pub. 2002/0152299) and further in view of Lewis et al. (U.S. Patent 6,233,565).

    a. *Referring to Claim 13:*

    As per Claim 13, Engberg et al. and Traversat et al. disclose the method according to claim 12, wherein said registering step comprises: entering the same random password on the pervasive device and the personal authentication gateway **[(lines 52-59, Col. 4; lines 15-19, Col. 5; lines 1-18, Col. 7 from Engberg et al.)]**.

    Engberg et al. do not expressly disclose the remaining limitations of the claim. However, Lewis et al. disclose generating on the personal authentication gateway an encryption key, Slave_ID_Secret, which is encrypted by the random password **[(lines 7-11, Col. 40 from Lewis et al.)]**;

    transferring the protected key to the pervasive device and computing a fingerprint of the protected key on the personal authentication gateway **[(lines 1-4, Col. 29 from Lewis et al.)]**; and comparing the fingerprint of the received and decrypted protected key on the pervasive device **[(lines 6-9, Col. 29 and lines 9-11, Col. 40 from Lewis)]**.

    Engberg et al. and Lewis et al. are from similar technology relating to security for the digital content and data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Engberg et al. with Lewis et al. to have hash of key for verification since one would be motivated to use said public and private keys of said client and server to perform the authentication (lines 15-16, Col. 6 from Lewis et al.). Therefore, it would have been obvious to combine Engberg et al. with Lewis et al. to obtain the invention as specified in claim 13.

b. *Referring to Claim 14:*

As per Claim 14, Engberg et al., Traversat et al., and Lewis et al. disclose the method according to claim 13, wherein the encryption key, Slave_ID_Secret, is used as a protection arrangement for token requests and token responses **[(lines 12-14, Col. 6 from Lewis et al.) and (lines 22-25 and 57-62, Col. 5 and from Engberg et al.)]**.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

   a. Goland (U.S. Pub 2003/0056114) discloses a branding process provides a networked computing device with initial set up information, including a name, a public/private key pair, and a set of certificates the device will need to inter-operate with other devices in the trust group. A branding device conveys the initial set-up information to the networked computing device via a limited access network interface, or alternatively via a broadcast network media with the device enclosed in a wave guide and/or Faraday cage. The networked computing device can then use the set up information to verify that other devices on the network that seek to interact with the device are also members of the trust group, with which networked computing device can interact.

b. Sasmazel et al. (U.S. Patent 6,725,376) disclose a distributed computer system and server architecture transmitting an electronic ticket over the system, such as the Internet, enabling a user to be authenticated and authorized for a requested operation. An "eticket" architecture (including identification information) is generated by, for example, an authentication server. The information in the eticket is hashed using, for example, a Message Digest Protocol, and a hash number is generated. The hash number is then encrypted by the authentication server using a private key, and the identification information in the eticket and the encrypted hash number are concatenated by the authentication server to generate a completed "eticket" architecture. The "eticket" may then be transmitted over the Internet (i.e., a non-secure environment) from server to server without having the information in the "eticket" altered, and without having to "reauthenticate" the user at each server.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Mar. 30, 2007

Thanhnga B. T
AU2135